UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,846	12/21/2001	Keith Alexander Harrison	30003039-2	5756

7590 09/22/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,846	HARRISON ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on June 09, 2006 has been entered. Claims 42-56 are pending. Claims 1-41 are cancelled by the applicant and claim 42 is also amended by the applicant. The examiner in charge is on medical leave. The present application has been reassigned to the present examiner, who has thoroughly reviewed and searched the instant invention.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 42-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic, U.S. Patent Number 5,745,574, hereinafter "Muftic", in view of Sweet et all, U.S.Patent Application Publication Number 2002/0031230, hereinafter "Sweet", and further in view of "Handbook of Applied Cryptography" by Menezes, hereinafter llMenezes".

Regarding claim 42, Muftic discloses a method of communicating credentials, the method comprising: a first party/u2 (fig. 4, #430), communicating a composite credential/certificate (fig. 3), across a distributed electronic network/Internet (col. 10, lines 35-37), to a second party/u1 (fig. 4, #450), wherein the composite credential/certificate, comprises a plurality of obfuscated credentials (fig. 3, #300-370).

Muftic lacks or does not expressly disclose in which different obfuscation is used for at least two credentials in the composite credential. However Sweet discloses in which different obfuscation is used for at least two credentials in the composite credential/file (paragraph 0143). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Muftic with the device of Sweet to use different obfuscation for at least two credentials in the composite credential because it facilitates differentiated role-based access to large

collections of digital information, as taught by Sweet, (paragraph 0143). Muftic further discloses the second party/u1, de-obfuscating/decrypting (fig. 5, #530 or #510) at least one credential (col. 12, lines 51-52), and the second party communicating to a third party/CA3 (fig. 4, #420), at least one obfuscated credential from the composite credential (col. 13, lines 13-16). Muftic is also silent on the capability to show that a certificate can be communicated from a CA as well as the user.

However, Menezes teaches a certificate may come from a user/trusted third party, (page 39, 1.1 1.3). One of ordinary skill in the ad would have been motivated to modify the method of Muftic with the method of Menezes to allow a certificate to come from a user because a trusted third party may have access to the secret or private keys of users and therefore send a certificate. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Muftic with the method of Menezes.

Regarding claims 43-45, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein the second party/u1, receives a composite credential/cedificate, and the second party/u1 , modifies the received composite credential/u1, before communicating it to the third party/CA3 (col. 12, lines 49-51), wherein the second party/u1, receives a composite credential/cedificate, and the second party/u1 communicates the received composite credential/cedificate, to the third pady/cA3 (fig. 4), wherein all credentials are obfuscated within the composite credential/cedificate (fig. 3).

Regarding claim 46, Muftic fudher discloses a method of communicating credentials according to claim 45 as modified above, in which different obfuscation is used for each obfuscated credential in the composite credential (Sweet, paragraph 0143).

Regarding claim 47, Muftic fudher discloses a method of communicating credentials according to claim 42 as modified above, wherein the composite credential/cedificate, comprises a first credential and a second credential in which the second credential is enveloped by the first credential (digest, col. 12, lines 54-56).

Regarding claim 48-50, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein the first party/u2, communicates to the second party/u1, an obfuscated composite credential/certificate, comprising a first credential and a second credential in which the second credential is enveloped by the first credential (digest, col. 12, lines 54-56), wherein the obfuscated composite credential/certificate, is de-obfuscated/decrypted, by the second party/u1, thereby to obtain the first credential and a party de-obfuscated/decrypted, second credential, which partly de-obfuscated/decrypted, second credential is communicated by the second party/u1, to a third party/CA3, wherein the third/CA3, party de-obfuscates/decrypts, the partly de-obfuscated second credential (col. 12, lines 56-60).

Regarding claim 51, Muftic further discloses a method of communicating credentials according to claim 50 as modified above, wherein the composite credential/cedificate, is at least partly obfuscated, and wherein the second party/u1, de-obfuscates a relevant credential (fig. 5, #530 or #510).

Regarding claim 52-55, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein at least one credential is digitally signed, in which a plurality of credentials is digitally signed, in which all credentials in the composite credential/certificate, are digitally signed, in which the composite credential/certificate, is digitally signed (col. 11, lines 36-38).

Regarding claim 56, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, in which the distributed electronic network is the Internet (col. 10, lines 35-37).

Response to Argument

4. Applicant's arguments filed June 9, 2006 have been fully considered but they are not persuasive.

Applicant argues that:

The combination of Muftic, Sweet, and Menzes fails to teach each and every element of claim 42 and request that the rejection be withdrawn. Further, applicant asserts that the rejection under 35 U.S.C. § 103 in view of Menzes is not

proper because the Examiner has not properly identified a suggestion or motivation in the prior art to modify either Muftic or Sweet with Menzes.

Examiner disagrees with the applicant and still maintains that:

Muftic does teach the method of communication between parties. In fact, Figure 4 of Muftic clearly shows the communication between the users U1 and U2 to verify transactions. In this example, assume that user U2 (430) sends a signed message to user U1 (450). It is convenient and preferred for each user, such as U1, to have certificates stored in their certificate storage data base 230, for themselves and for each station between the user U1, and the policy registration authority (column 12, lines 1-6 of Muftic). Furthermore, Security services for applications and users in the network are facilitated by a set of common certification functions accessible by well-defined application programming interface which allows applications to be developed independently of the type of underlying hardware platforms used, communication networks and protocols and security technologies (Muftic's abstract). However, Muftic is silent on the capability of showing different obfuscation is used for at least two credentials in the composite credential. However Sweet discloses in which different obfuscation is used for at least two credentials in the composite credential/file (paragraph 0143). The combination of teaching between Muftic and Sweet is also silent on the capability to show that a certificate can be communicated from a CA as well as the user.

However, Menezes teaches a certificate may come from a user/trusted third party, (page 39, 1.1 1.3). One of ordinary skill in the ad would have been motivated to modify the method of Muftic with the method of Menezes to allow a certificate to come from a user because a trusted third party may have access to the secret or private keys of users and therefore send a certificate. Thus, the combination of teaching between Muftic, Sweet, and Menezes teaches the claimed subject matter.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teaching between Muftic, Sweet, and Menezes is proper and sufficient.

Besides, applicant further argues that because of the composite credentials, direct communication between the first party and third party claimed in claim 42 is unnecessary. Examiner finds this statement of applicant is very indefinite and does not even address in claim 42.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., because of the composite credentials, direct communication between the first party and third party claimed in claim 42 is unnecessary) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

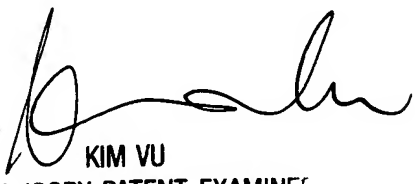
5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.



KIM VU
SORY PATENT EXAMINER
OLOGY CENTER 2100

TBT
September 18, 2006